

Appl. No. 09/751,899  
Amdt. Dated 02/06/2006  
Reply to Office Action of 12/06/2005

### REMARKS

This Amendment is in response to the Office Action mailed December 6, 2005. In the Office Action, claims 1-23 were rejected under 35 U.S.C. §103(a). Claims 12-14 have been cancelled without prejudice. Applicant respectfully traverses the §103(a) rejections and respectfully requests the Examiner to withdraw these rejections.

#### *Rejection Under 35 U.S.C. § 103*

Claims 1-14 and 22-23 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis (U.S. Patent No. 6,425,084) in view of Adams (U.S. Patent No. 6,363,485). Moreover, claims 15-21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis in view of Adams and Lohstroh (U.S. Patent No. 5,953,419). Applicant respectfully traverses these rejections in their entirety because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. See *MPEP* §2143; see also *In Re Fine*, 873 F. 2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). Herein, at a minimum, the combined teachings of the cited references do not describe or suggest all the claim limitations set forth in independent claims 1, 15 and 21.

#### A. §103(A) REJECTION OF CLAIMS 1-14 AND 22-23

Claims 1-14 and 22-23 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis (U.S. Patent No. 6,425,084) in view of Adams (U.S. Patent No. 6,363,485). Applicant respectfully submits that a *prima facie* case of obviousness has not been established because neither Rallis nor Adams, alone or in combination, suggests every limitation set forth in the above-identified claims.

Appl. No. 09/751,899  
Amdt. Dated 02/06/2006  
Reply to Office Action of 12/06/2005

For instance, with respect to independent claim 1, the Office Action states that column 3, lines 18-29 and column 5, lines 9-21 of Rallis teach an operation of “releasing a first keying material from a token communicatively coupled to the platform in response to authenticating the user.” *See Page 3 of the Office Action.* Applicant respectfully disagrees with these findings because Rallis teaches the boot-up user-validation program where a key device serial number, considered by the Examiner to constitute the “first keying material” as claimed, is released *prior to* user authentication. This key device serial number is *not released in response to authenticating the user* as claimed. *Emphasis added.* Adams also fails to suggest this limitation as well.

Moreover, the Office Action states that Rallis teaches an operation to “decrypt a second BIOS area to recover a second segment of BIOS code.” *See Page 3 of the Office Action.* Applicant respectfully disagrees. First, the limitation has been improperly parsed because claim 1 states “*using the combination key to decrypt a second BIOS area to recover a second segment of BIOS code.*” *Emphasis added.* There is no teaching by the combination of Rallis and Adams in using a combination key, the first keying material combined with a second keying material internally stored within the platform, to decrypt a second BIOS area to recover a second segment of BIOS code.

Secondly, the Office Action states that the decryption of validation records, apparently considered to be the second BIOS area, is taught by Rallis (see Page 3 of Office Action). However, the validation records do not constitute the second BIOS area. Validation records of Rallis are stored in a reserved sector of the hard disk (42), not BIOS ROM (30). Moreover, neither Rallis nor Adams, alone or in combination, suggest using a combination key being the first keying material (key device serial number) combined with a second keying material internally stored within the platform in order to decrypt the second BIOS area (validation record) to recover a second segment of BIOS code. The fields of the validation records include the key device serial number, PIN, an internal device serial number, a level parameter, encrypted keys and user information. No BIOS code is stored in the validation programs.

Appl. No. 09/751,899  
Amdt. Dated 02/06/2006  
Reply to Office Action of 12/06/2005

Hence, since neither Rallis nor Adams describe or suggest all of the claim limitations set forth in independent claim 1, a *prima facie* case of obviousness has not been established, and thus, the §103(a) rejection should be withdrawn.

Based on the dependency of claims 2-11 on independent claim 1, believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traverse is warranted. Applicant reserves the right to present such arguments in an Appeal is warranted. Withdrawal of the §103(a) rejection as applied to claims 1-11 is respectfully requested.

**B. §103(A) REJECTION OF CLAIMS 15-21**

Moreover, Claims 15-21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis in view of Adams and Lohstroh (U.S. Patent No. 5,953,419). Applicant respectfully submits that a *prima facie* case of obviousness has not been established because neither Rallis, Adams nor Lohstroh, alone or in any combination, suggest every limitation set forth in the above-identified claims.

With respect to independent claims 15 and 19, Applicant incorporates the arguments set forth above in which the trusted platform module produces a combination key by combining a first incoming keying material *released after authentication of a user of the platform* with a second keying material. *Emphasis added.* In contrast and teaching away from the claimed invention, the teachings of Rallis are directed to the release of the first keying material (key device serial number) *as part* of the user authentication procedure, not the release of the first keying material after *authentication of a user of the platform* as claimed. *Emphasis added.*

In conclusion, the new combination of the teachings of Lohstroh in order to modify the teachings of Rallis (and Adams), namely modifying when first incoming keying material is released, is impermissible. The Federal Circuit has consistently held that the combination of references in support of a §103 rejection is improper when such combination is directed to the modification of an invention disclosed and it destroys the intent, purpose or function of the invention disclosed. See *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). *MPEP*

Appl. No. 09/751,899  
Amdt. Dated 02/06/2006  
Reply to Office Action of 12/06/2005

§2143.01. With respect to Rallis, the release of the key device serial number must occur during the authentication procedure, not after the procedure.

Hence, withdraw of the outstanding §103(a) rejection as applied to independent claims 15 and 19 as well as claims 16-18 and 20-21 dependent thereon is respectfully requested.

**Conclusion**

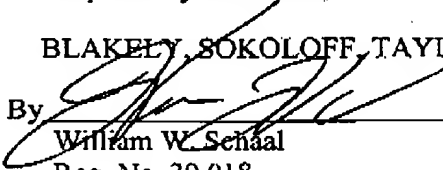
Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 2/6/06

By

  
William W. Schaal

Reg. No. 39,018

Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor  
Los Angeles, California 90025

**CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.81)**

I hereby certify that this correspondence is, on the date shown below, being:

**MAILING**

☐ deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.

**FACSIMILE**

☒ transmitted by facsimile to the Patent and Trademark Office.

Date: 2/6/2006

  
Nicole Erquiaga

2/6/2006

Date